

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 63-063232

(43)Date of publication of application : 19.03.1988

(51)Int.Cl.

H04L 9/00

(21)Application number : 61-206855

(71)Applicant : OKI ELECTRIC IND CO LTD

(22)Date of filing : 04.09.1986

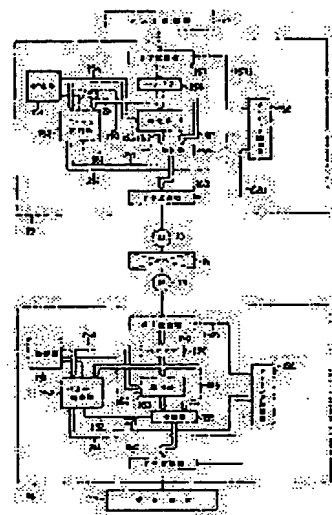
(72)Inventor : SAKAMOTO SHUNICHIRO

## (54) CIPHERED COMMUNICATION SYSTEM

## (57)Abstract:

PURPOSE: To cipher even a packet switching network by ciphering from the next byte of a telegram through its end only when pattern data in the telegram agrees with pattern data which is set and inputted to an input means.

CONSTITUTION: Telegram data from a host computer 11 is set to a buffer 156 through an SP converter 157. Telegram data from the buffer 156 is inputted to a pattern detector 152, a ciphering device 153 and a switch 159. Without a switching signal from the pattern detector 152, the switch 159 outputs not-ciphered telegram data that is inputted through a data line 163, and transmits it to a line (a network 14) through a MODEM 13. When the pattern detector 152 detects that both pattern data are the same, the switching signal is outputted through a signal line 161, and the switch 159 selects an output line 162 from the ciphering device 153. The ciphering device 153 ciphers data from the host computer 11, and an PS converter 160 transmits it to the MODEM 13 and the network 14 through the switch 159. 12 terminal equipment 151 setting device 158 timing control part 164 decoding device.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

⑬ 日本国特許庁(JP)

⑭ 特許出願公開

⑯ 公開特許公報(A)

昭63-63232

⑮ Int.Cl.<sup>4</sup>

H 04 L 9/00

識別記号

庁内整理番号

Z-7240-5K

⑰ 公開 昭和63年(1988)3月19日

審査請求 未請求 発明の数 1 (全15頁)

⑱ 発明の名称 暗号化通信方式

⑲ 特 願 昭61-206855

⑳ 出 願 昭61(1986)9月4日

㉑ 発 明 者 坂 本 俊 一 郎 東京都港区虎ノ門1丁目7番12号 沖電気工業株式会社内  
㉒ 出 願 人 沖電気工業株式会社 東京都港区虎ノ門1丁目7番12号  
㉓ 代 理 人 弁理士 鈴木 敏明

明 細 書

1. 発明の名称

暗号化通信方式

2. 特許請求の範囲

回線における電文データを暗号化して通信する暗号化通信方式において、

パターンデータを設定して入力するための入力手段と、

前記電文データ中のパターンデータと前記入力手段に設定入力されたパターンデータを比較する比較手段と

を備え、

前記比較手段で前記パターンデータが互いに一致したときに、前記電文データ中の前記パターンデータの次のバイトデータから終了のバイトデータまでを暗号化して通信する

ことを特徴とする暗号化通信方式。

3. 発明の詳細な説明

(産業上の利用分野)

本発明は通信回線における電文データの秘密保護に係り、特にこの電文データを暗号化して通信する暗号化通信方式に関するものである。

(従来の技術)

従来、このような分野の技術としては、例えば特開昭58-213544号公報に示されるものがあった。このような従来装置においては、回線上を流れるデータの保護のため暗号装置を回線に入れることが行なわれている。

第2図は回線における電文データを暗号化する場合に適用されている従来システムの接続図である。暗号装置1はホスト計算機2とモデム4の間および端末装置3とモデム4の間に設けられる。なお、同図において、モデム4の間に設けられているのは交換網5である。通常この型の暗号装置は、回線が接続されると送受信データ(電文データ)を常に暗号化/復号化するようにしている。

第14図は送信電文(同図(a))と、暗号電

文(同図(b))と、それを復号した受信電文(同図(c))の構成例を示す図である。この例では、最初のフレームのA部(アドレスフィールド)以後をすべて暗号化している、すなわち、ホスト計算機2あるいは端末装置3からの送信電文(第14図(a)図示)を送信側の暗号装置4で最初のA部から暗号化し、回線へは暗号電文(第14図(b)図示)を送出している。この暗号電文を受信した受信側の暗号装置4はこれを復号化して受信電文(第14図(c)図示)とし、これをホスト計算機2あるいは端末装置3に渡している。

このため、回線の種類が専用回線、公衆回線等であっても、一度接続されると電文データの内容にかかわらず送信データをそのまま伝送する回線に対しては、従来の暗号装置を適用することは可能である。しかし、例えばパケット交換網のパケット交換サービスを利用しようとした場合には、網に対して接続手順(X25、CALL)およびデータ転送手順(X25、DATA)を行う必要

がある。この手順では、第15図に示す様にパケット内のパケットヘッダに制御情報があり、このパケットを網との間でデータをやり取りすることにより通信が行なわれている。

ところが、従来の暗号装置における暗号化通信方式では、第14図(b)に示す様に暗号化開始後はすべてのF部(フラグ)、A部(アドレスフィールド)、C部(コントロールフィールド)、データ部を暗号化してしまうため、網において接続手順、データ転送手順に必要なデータを認識することが出来ない。このため、従来の暗号化通信方式をパケット交換網に適用することができないという問題があった。

そこで本発明は、パケット交換網等の如く、網と端末/ホストとの間で接続手順、データ転送手順がある場合にも適用可能な暗号化通信方式を提供することを目的とする。

(問題点を解決するための手段)

本発明に係る暗号化通信方式は、所定のパターンデータを設定入力する入力手段と、電文データ

中のパターンデータと入力手段に設定入力されたパターンデータを比較する比較手段とを備え、比較手段でパターンデータが互いに一致したときに電文データ中のパターンデータの次のバイトデータから終了のバイトデータまでを暗号化して通信すること特徴とする。

(作用)

本発明の暗号化通信方式は以上のように構成されるので、入力手段は監視のためのパターンデータを設定入力するように働き、比較手段は監視のために設定入力されたパターンデータと送られる電文データ中のパターンデータを比較し、暗号化して通信されるデータが否かを監視するように働き、従って比較手段における比較結果にもとづいて暗号化すべきデータのみを暗号化して通信するように働く。

(実施例)

以下、添付図面の第1図、第3図ないし第13図を参照して本発明のいくつかの実施例を説明する。

第1図は本発明の第1の実施例に係る暗号化通信方式を適用する通信システムの構成図である。同図において、ホスト計算機11と端末装置12の間の通信は、2つのモデム13とこれらの間に接続される網14を介してなされる。また、ホスト計算機11側には本実施例の要部をなす暗号装置の暗号化部15が接続され、端末装置12側には同じく本実施例の要部をなす復号化部16が接続される。なお、第1図はホスト計算機11から端末装置12への通信の例を示しており、従って端末装置12からホスト計算機11への通信を行なう場合には、上記と同様のものを逆方向に配置すればよい。

次に、暗号化部15の構成を第1図に従って説明する。暗号化部15はパターンデータと暗号化キーを設定するための設定器151を有し、ここで設定されたパターンデータは信号線154を介してパターン検出器152および暗号器153に与えられる。また、暗号化部15はホスト計算機11からのシリアルな電文データをパラレル信号

に変換するためのSP変換器157と、ここで変換された電文データを一時記憶するバッファ156を有し、バッファ156の内容は信号線29を介してパターン検出器152に与えられると共に、信号線163を介して暗号器153および切替器159に与えられる。

切替器159は暗号器153からの暗号化されたデータを信号線162を介して受けると共に、バッファ156から送信された暗号化されていないデータを信号線163を介して受ける。そして、切替器159はパターン検出器152からの信号線161による出力に応じてこれらデータを切り替え、暗号化されたデータ又は暗号化されていないデータのいずれかをPS変換器160に出力する。タイミング制御部158はSP変換器157からの信号を信号線1571を介して受け、信号線214によるバイトクロックと信号線221による電文中信号でパターン検出器152の動作を制御すると共に、信号線1581を介してPS変換器160の動作タイミングをも制御する。

27に与えられると共に、パターンデータメモリ21にも与えられる。さらに、設定器154からのパターンデータは信号線154を介してパターンデータメモリ21のデータ入力端子に与えられる。

カウンタ22はORゲート27の出力信号をカウントし、信号線221からの電文中信号によりリセットされる。そして、カウンタ22は出力をパターンデータメモリ21のアドレス入力端子Aに与える。パターンデータメモリ21は信号線155からのパターンデータ書込信号に応じて信号線154からのパターンデータを入力する。そして、データ線211によりマスクデータをANDゲート23に与えると共に、データ線212を介して比較データを比較器24に与える。また、パターンデータメモリ21は信号線213を介して終了信号をANDゲート26に与えると共に、これをインバータを介してANDゲート215に与える。F/F25の出力は信号線251を介してANDゲート26に与えられ、

次に、復号化部16の構成を第1図に従って説明する。復号化部16の構成は暗号化部15の構成と基本的に同一である。異なる点は、暗号器153に代えて復号器164が設けられていることのみである。

次に、第3図を参照して第1図に示すパターン検出器152の詳細な構成を説明する。このパターン検出器152はパターンデータメモリ21と、カウンタ22と、ANDゲート23と、比較器24と、フリップフロップ(F/F)25とを主たる構成要素とする。

まず、第1図に示すバッファ156からの暗号化されていない電文データは信号線29を介してANDゲート23に与えられる。第1図中のタイミング制御部158からの電文中信号は信号線221を介してカウンタ22およびF/F25の反転入力端子に与えられ、バイトクロックは信号線214を介してANDゲート215に与えられる。第1図中の設定器151からのパターンデータ書込信号は信号線155を介してORゲート

ANDゲート26の出力は切替信号として信号線28から第1図の切替器159に与えられる。

第4図は第3図に示すパターンデータメモリ21の詳細構成図である。図示の如く、パターンデータメモリ21は17ビット×nワード構成の書込可能なメモリを使用し、上位8ビットをマスクデータM、次の8ビットを比較データC、最後の1ビットを終了フラグとして使用している。

次に、第5図を参照して第1図に示す暗号器153の詳細な構成を説明する。同図(a)の如く、暗号器153は暗号化キーがK1からK4までの4個のキーレジスタ31と、4個のEXOR回路32と、 $f_1$ から $f_3$ までの3個の換字用ROM34を主たる要素とする。第5図(b)、(c)は換字用ROM34の構成の一例を示すもので、アドレスが8ビット、データが8ビットの計256バイトのROMである。このような換字変換ROM34によれば、例えば第5図(c)の様にデータを囲き込んでおくことにより、アドレスの00はデータの01へ、アドレスの01はデ

ータのE4へと換字変換される。

このように構成される暗号器153によれば、入力された平文データ(暗号化されていないデータ)はEXOR回路32でキーレジスタ(K1)31のキーK1と排他的論理和がとられる。次に、換字用ROM( $f_1$ )34で換字変換され、さらにキーレジスタ(K2)31のキーK2と排他的論理和がとられる。以下同様にして、最終的にはキーレジスタ(K4)31のキーK4と換字用ROM( $f_4$ )34の出力との排他的論理和が暗文データ(暗号化されたデータ)となる。

第1図に示す復号器164の構成も上記暗号器153と同様で、暗文データと平文データの流れる方向を逆にすれば良い。

次に、上記の如く構成される第1の実施例に係る暗号化通信方式を適用した装置の作用を説明する。

まず、暗号化通信動作をさせる前には暗号装置を初期設定する必要がある。この初期設定は次のように行なう。すなわち、第1図の設定器151

によりパターン検出器152内のパターンデータメモリ21にマスクデータM、比較データC、終了フラグを設定し、つぎに暗号器153の4個のキーレジスタ31にそれぞれ暗号キーK1、K2、K3、K4を設定する。同様に、端末装置12側の復号化部16のパターン検出器152、復号器163にも上記と同様の設定をする。

上記の初期設定が終わると、次にパターンデータの設定を行なう。これは、例えば第6図および第7図に示すように行なう。すなわち、第6図(a)に示す送信電文中のD<sub>1</sub>~D<sub>5</sub>の部分のみを暗号化する場合には、第7図に示すパターンをパターンデータメモリ21に設定する。このようにすると、暗号化された暗号電文は第6図(b)に示すようになり、復号化された受信電文は第6図(c)に示すようになる。

次に、暗号化/復号化動作を説明する。まずホスト計算機11からの電文データはSP変換器157によりバイト単位のデータに変換される。このとき、第6図に示す同期パターン(F)、フ

レームチェックシーケンス(FCS)は除去される。

次に、SP変換器157から最初のデータがバッファ156にセットされ、制御線1571によりタイミング制御部158にデータ受信開始を通知する。タイミング制御部158は信号線221、214を介してパターン検出器152へ電文中信号とバイトクロックを出力する。

次に、バッファ156からの電文データはパターン検出器152、暗号器153および切替器159にそれぞれ入力される。パターン検出器152からの切替信号(信号線161)がないときは、切替器159はデータ線163を介して入力される暗号化されない電文データを出力している。切替器159の出力はPS変換器160によりシリアル変換され、同期パターン(F)、フレームチェックシーケンス(FCS)を付加されてモデム13を介して回線(網14)に送出される。

パターン検出器152から信号線161を介して切替信号が出力されるまでは、PS変換器

160へはバッファ156のデータがそのまま与えられる。パターン検出器152によりパターンデータの一致が検出されると、信号線161を介して切替信号が出力され、切替器159は暗号器153からの出力線162を選択する。この後、ホスト計算機11からのデータは暗号器153により暗号化され、切替器159を介してPS変換器160によりモデム13、網14に送信される。

ホスト計算機11からの電文データ出力の終了はSP変換器157で検出され、制御線1571によりタイミング制御部158に通知される。タイミング制御部158はパターン検出器152への信号線221による電文中信号をOFFとしてパターン検出動作をリセットし、制御線1581により電文データの終了をPS変換器160に通知する。PS変換器160では電文データの終了としてフレームチェックシーケンス(FCS)、終結フラグを付加し、電文データの送出を終了する。

端末装置12側の復号化部16においても以上

説明したと同様に動作するが、バッファ156の出力を復号器164を通して切替器に入力することのみ異なっている。

次に、上記作用におけるパターン検出器152の動作を、第3図、第6図および第7図を用いて説明する。なお、第6図(a)の送信電文の5.1部分は、すでにパターンデータメモリ21に書き込まれているものとする。

最初のバイトA部がSP変換器157からバッファ156にセットされると、タイミング制御部158から信号線221、214を介して電文中信号とバイトクロックがパターン検出器152に出力される。信号線214のバイトクロックはSP変換器157でバイト単位に変換されるたびに制御信号線1571を通じてタイミング制御部158に入力され、そこからパターン検出器152に入力される。

カウンタ22は信号線221の電文中信号によりリセットが解除され、パターンデータメモリ21のアドレス入力端子Aにアドレス0を出力し

ている。パターンデータメモリ21のアドレス0の内容のうち、マスクデータM=FFはデータ線211に、比較データC=55はデータ線212に、終了フラグ=0は終了信号線213に出力されている。この状態で、バッファ156から信号線29を介して電文データがANDゲート23に入力される。このANDゲート23で、データ線211からのマスクデータMと論理積が取られ、この場合はマスクデータMがFFであるので信号線(データ線)29の電文データがそのまま比較器24に入力される。

比較器24ではパターンデータメモリ21の比較データC(信号線212からのデータ)と比較され、その結果が信号線241を介してORゲート27に出力される。信号線241には両者が一致した場合に0が出力され、一致しない場合に1が出力される。F/F25とORゲート27はこの状態を記憶している。すなわち、比較器24の出力線241が0であればF/F25の出力線251は1のままであるが、1度でも比較器24

の出力線241が1となるとF/F25の出力線251は0となる。

ここで、第1バイトが一致した場合はF/F25の出力線251は1となっているが、パターンデータメモリ21の終了信号線213は0であるため、ANDゲート26によりゲートされて切替信号は信号線28を介して出力されない。

次に、第2バイトの受信時は、信号線214のバイトクロックによりORゲート27を通してカウンタ22にクロックが与えられ、カウンタ22の出力はアドレス1を示すことになる。これにより、パターンデータメモリ21のアドレス1の内容と信号線29の電文データが比較されることになる。以下同様にして、各電文データと比較される。

ここで第6バイト目の比較時には、パターンデータメモリ21のアドレス部にアドレス5が入力されている。この場合、パターンデータメモリ21の終了信号線213は1であるため、F/F25の出力線251が1であればANDゲート

26が開き、切替信号が信号線28を介して出力される。つまり、ここまでの電文データがすべて一致していれば、終了信号線213が1になったとき切替信号が信号線28から出力される。これにより以降のデータは暗号化されることとなる。

また、終了信号線213が1になるまでに電文データが1バイトでも不一致であると、F/F25の出力線251が0となるため切替信号は信号線28を介して出力されることがない。このため、それ以降も暗号化されない電文データが送信される。また、この終了信号線213によりANDゲート215を閉じて以降のバイトクロックをゲートする。

この様にして各電文データを比較し、パターンデータの一致した電文データの次のバイトから電文の終了までを暗号化する。マスクパターンMは電文データ中の通番等、各電文データ毎に変化するものをマスクするのに使用する。

この第1の実施例ではホスト/端末とモデムの間に暗号装置を設け、電文の一部のみの暗号化を

行なっている。このため、ホスト／端末からの電文を一度シリアルパラレル変換し、暗号化の後に再度パラレルシリアル変換している。ところが、以下に示す第2の実施例は、暗号機能を通信制御装置中にもたせている。

第8図乃至第13図を参照して、本発明の第2の実施例を説明する。

第8図は本発明に係る暗号化通信方式の第2の実施例に適用される通信制御装置の構成を示すブロック図である。通信制御装置80は制御用プロセッサ(μP)81と、このプロセッサ81に付設される制御メモリ(CM)82と、チャンネルインタフェース83aと、このチャンネルインタフェース83aに付設されるチャンネルバッファ83bと、データメモリ(DM)84と、暗号／復号器(CIP)85と、設定器86と、4個の回線ユニット(LA#0～LA#3)87とを有し、これらの間ではバスを介して互いにデータの授受ができるようになっている。

第9図は上記第2の実施例で用いられる回線コ

ントロールメモリの構成図である。そして、このメモリは各回線毎に設けられている。このメモリの内容は、通信制御用データ91と、暗号処理用データ92と、復号処理用データ93とを有している。

通信制御用データ91は従来の通信制御装置のものと同様で、通信速度、同期方式等の回線の情報である。このデータは第8図に示すCPUにより設定される。暗号処理用データ92はこの回線の送信データを暗号化するか否かのECフラグと、現在暗号化中であることを示すEIフラグと、暗号化キーEKEY0～EKEY3と、暗号化する電文データであるか否かを判定するためのマスクデータおよび比較データと、その管理用ポインタEP、EMとからなる。このうち、EC、EKEY0～EKEY3、EM、暗号マスクデータ、復号比較データは第8図における設定器86により設定される。EI、EPの初期値は0である。

復号処理用データ93はこの回線の受信データ

を復号するか否かのフラグDCと、現在復号化中であることを示すフラグDIと、復号化キーDKEY0～DKEY3と、復号化する電文データであるか否かを判定するためのマスクデータおよび比較データと、その管理用ポインタDP、DMとからなる。このうちDC、DKEY0～DKEY3、DM、復号マスクデータ、復号比較データは第8図の設定器86により設定される。またDI、DPの初期値は0に設定される。

第10図は第8図に示す暗号／復号器85の詳細な構成図である。暗号化キーレジスタ101はEKEY0～EKEY3、の4個からなり、暗号化キーレジスタ101へのセット信号は信号線102から与えられる。暗号化用データラッチ103と、 $f_1 \sim f_3$ の3個の暗号換字ROM105は排他的論理和手段104に結ばれ、最後の排他的論理和出力は暗号化データ出力用のゲート106を介して出力される。

復号化キーレジスタ107はDKEY0～DKEY3の4個からなり、復号化キーレジスタ

107へのセット信号は信号線108を介して与えられる。復号化用データラッチ109と $f_3 \sim f_1$ の3個の復号換字ROM110は排他的論理和手段104により結ばれ、最後の排他的論理和出力は復号化データ出力用のゲート111を介して出力される。

ここで、復号換字ROM110は暗号換字ROM105の逆変換を行なう内容をもっている。

次に、第8図乃至第10図に示す第2の実施例の作用を説明する。

第11図は第8図に示す通信制御装置におけるデータの処理を示すフローチャートである。この処理は、第8図に示す制御プロセッサ81が制御メモリ82に書き込まれた内容に従って動作することにより行なわれる。

制御用プロセッサ81は動作開始後、チャンネル要求チェック(ステップ301)とLA要求チェック(ステップ303)を常に行なっている。チャンネル要求チェック(ステップ301)で要求有りの場合には、チャンネルコマンド処理(ステップ

302)へ行きCPUからのコマンド(例えば送信要求、受信要求)の処理を行なう。LA要求チェック(ステップ303)で要求チェック有りの場合には、LA選択(ステップ304)でどの回線ユニットLAからの要求かを判別し、第9図に示す回線コントロールメモリのアドレスを得る。

次に、送信/受信チェック(ステップ305)でLAからの要求が送信か受信かを判別し、送信の場合には送信終了チェック(ステップ305)で送信データがすべて送信し終わったかどうか判断する。終了であった場合には、送信終了処理(ステップ308)でLAに対する終結処理(例えばフレームの終了)と回線コントロールメモリのイニシャライズを行う。終了でなかった場合には、LA出力(ステップ307)で第8図に示すチャネルインタフェース83aに付設されたチャネルバッファ83bからLAへデータを出力する。このとき、後述の方法によりデータを暗号化するか否かの判断と暗号化処理を行なう。

送信/受信チェック(ステップ305)におい

て受信要求であった場合には、受信終了チェック(ステップ309)で受信が終了したかどうかの判別を行う。終了であった場合には、受信終了処理(ステップ311)でLAすなわち回線ユニットのリセットと回線コントロールメモリの初期化を行い、終了でなかった場合にはLA入力(ステップ310)でLAからデータを読み出し、第8図に示すチャネルインタフェース83aに付設されたチャネルバッファ83bのデータをセットする。このとき、そのデータを復号化するか否かの判別を行うと共に、復号化する場合にはその復号処理を行なう。

第12図は第11図のLA出力処理(ステップ307)およびLA入力処理(ステップ310)の詳細を示すフローチャートである。

まず、LA出力について第12図(a)を参照して説明する。LA出力はステップ401でチャネルバッファ83bから送信データを取り出すことにより始まる。

次に、暗号化する送信データであるか否かを示

すECビットをチェックする(ステップ402)。そして、EC=0である場合には、この回線は暗号化を行なわない回線としてステップ413に行き、送信データをそのままLAにセットする。EC=1でかつEI=1の場合には暗号化を適用する回線として、ステップ412で送信データを暗号化した後、ステップ413でLAにセットする。

ステップ403でEI=0の場合には、次のステップ404で管理用ポインタEPとEMを比較する。そして、EP=EMであった場合にはこの電文はすでに暗号化対象外であると判別されているので、送信データをそのままLAにセットする(ステップ413)。ステップ404でEP≠EMの場合には、ステップ405でまずEPの指すマスクデータと比較データを、第9図の回線コントロールメモリ内の暗号処理用データ92から得る。

ステップ406で送信データとマスクパターンとの論理積を取り、ステップ407でその値と比

較データを比較する。一致しない場合はEPをEMの値とし(ステップ408)、この電文を暗号対象外として送信データをLAにセットする(ステップ413)。一致した場合にはEPに1を加算し(ステップ409)、再度EPとEMを比較する(ステップ410)。

ステップ410でEPとEMが一致の場合には、第9図の暗号処理用データ92内の比較データがすべて一致したことになり、EIフラグを1にセットし(ステップ411)、次の送信データから暗号化を行う。不一致の場合にはステップ411の処理を行わず、LAに送信データをセットする(ステップ413)。

この様にして送信電文の比較チェックを行ない、一致検出後の電文データのみ暗号化を行なう。電文データの終了時は第11図のステップ308の送信終了処理でEIフラグおよびEPを0にリセットし、次の電文チェックを可能にする。

LA入力の処理は第12図(b)に示す通りであるが、第12図(a)のLA出力処理と略同一



である。すなわち、LA入力ステップ414のLAからのデータ入力処理と、ステップ415の復号処理と、ステップ416のチャンネルバッファへの受信データセットがLA出力処理と異なるのみで、EC、EI、EP、EMをそれぞれDC、DI、DP、DMと読み替えれば全く同様の処理である。

第13図は第12図(a)に示す暗号化処理(ステップ412)と、同図(b)に示す復号化処理(ステップ415)の詳細は処理を示すフローチャートである。

第13図(a)の暗号化処理ではまず、ステップ501で暗号化キーレジスタ101へ第9図の暗号処理用データ92のEKEY0~EKEY3をセットする。次に、ステップ503で暗号化したいデータを第8図の暗号化用データラッチ103にセットする。これにより第5図で説明したと同様にして、暗号化されたデータが暗号化データ出力ゲートに出力される。そして、ステップ504で暗号化出力ゲート106からデータを読

む。

同様に第13図(b)の復号化処理においても、ステップ505で復号化キーレジスタ107へ復号処理用データ93のDKEY0~DKEY3をセットする。次に、ステップ503で復号化したいデータを第8図の復号化用データラッチ109にセットする。そして、ステップ507で復号化されたデータを復号化データ出力ゲート111から読み出す。

本発明は上記第1および第2の実施例に限定されるものではなく、種々の変形が可能である。例えば第1図、第3図、第5図の等の回路構成は一例であって、各要素のは他の要素で置換することができる。

(発明の効果)

以上、詳細に説明した様に本発明によれば、暗号化する電文の監視のためのパターンデータを入力する入力手段を設け、電文中のパターンデータが上記入力手段に設定入力されたパターンデータと一致した場合のみその電文の次のバイトから電

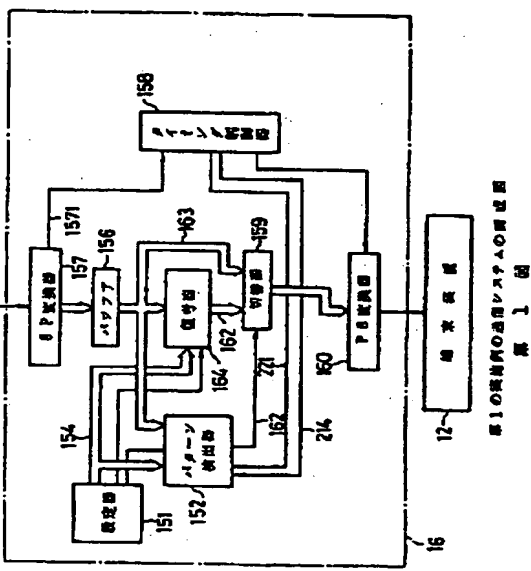
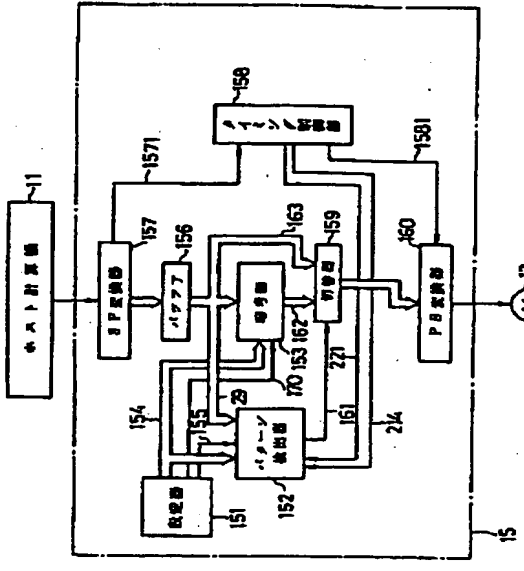
文の終了までを暗号化する様にしたので、網との間で手順に必要なデータ部はそのまま平文で網に通知することが可能となり、従って網と端末/ホストとの間で手順を必要とするバケット交換網に対しても暗号化を適用することができる。

#### 4. 図面の簡単な説明

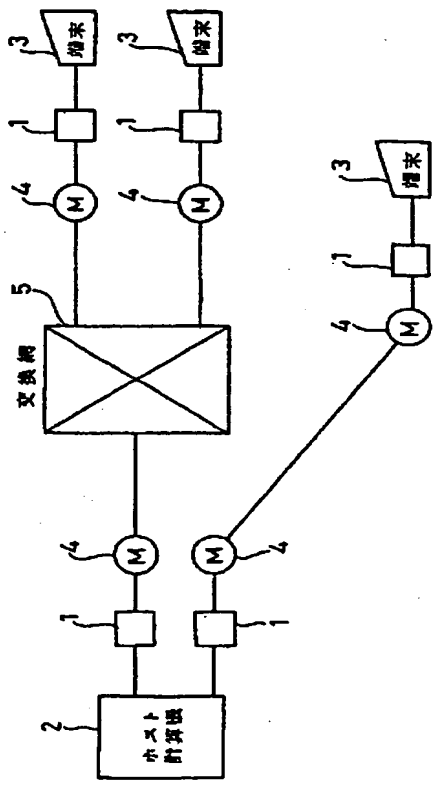
第1図は本発明方式の第1の実施例に係る暗号化通信方式を備えた通信システムの構成図、第2図は従来の暗号化通信方式を備えた通信システムの接続形態を示す構成図、第3図は第1図に示すパターン検出器の詳細な構成を示す図、第4図は第3図に示すパターンデータメモリの詳細な構成図、第5図は第1図に示す暗号器の詳細な構成図、第6図は第1の実施例による送受信電文と暗号化電文の構成図、第7図は第4図のパターンデータメモリに設定されるパターンデータの説明図、第8図は本発明方式の第2の実施例に係る暗号化通信方式を備えた通信システムの構成図、第9図は第2の実施例に用いられる回線コントロールメモ

リの構成図、第10図は第8図に示す暗号/復号器の詳細な構成図、第11図は第8図の装置におけるデータ処理を示すフローチャート、第12図は第11図のLA出力処理およびLA入力処理の詳細を示すフローチャート、第13図は第12図の暗号化処理と復号化処理の詳細を示すフローチャート、第14図は従来方式による送受信電文と暗号電文の構成図、第15図はバケットの構成図である。

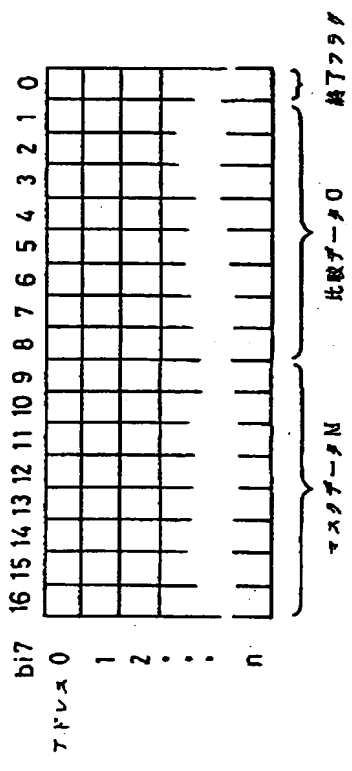
15…暗号化部、16…復号化部、31…キーレジスタ、32…EXOR回路、34…換字用ROM、80…通信制御装置、81…制御用プロセッサ、82…制御メモリ、83a…チャンネルインタフェース、83b…チャンネルバッファ、84…データメモリ、85…暗号/復号器、87…回線ユニット、101…暗号化キーレジスタ、104…排他論理和手段、105…暗号換字ROM、107…復号化キーレジスタ、110…復号換字ROM。



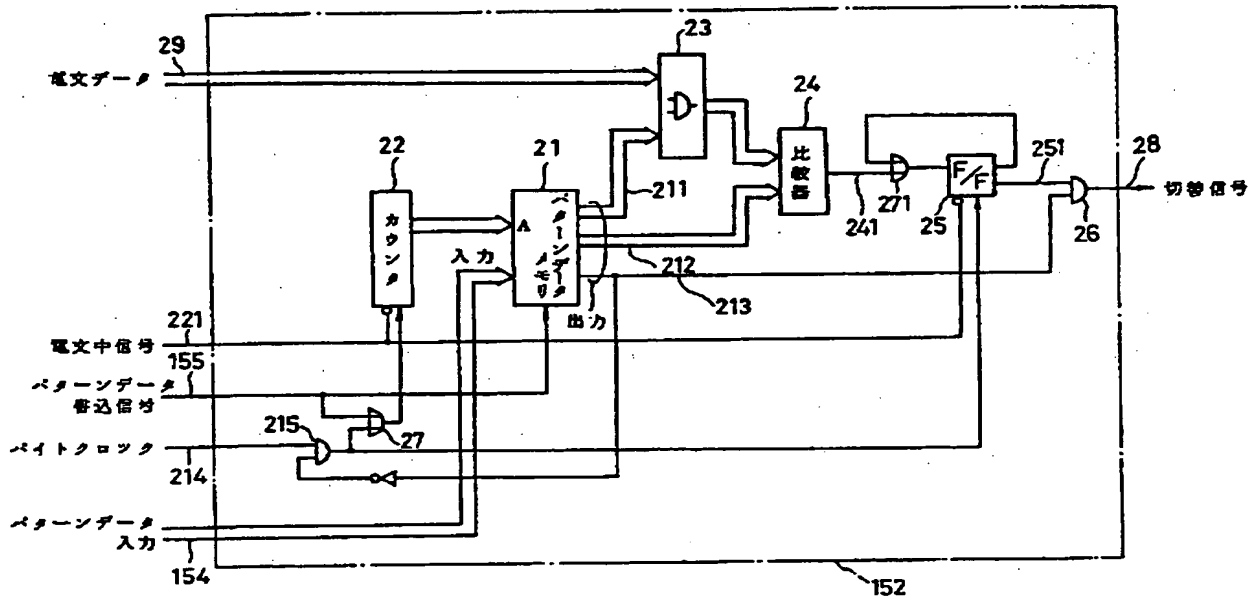
第10図の回路図のブロック図  
第1図



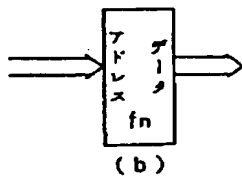
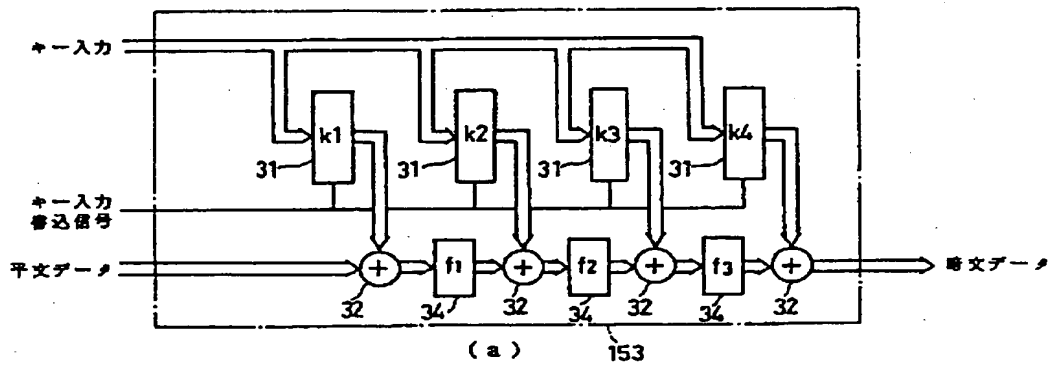
従来方式による場合の接続形態を示す図  
第2図



第3図のパターンデータメモリの構成図  
第4図



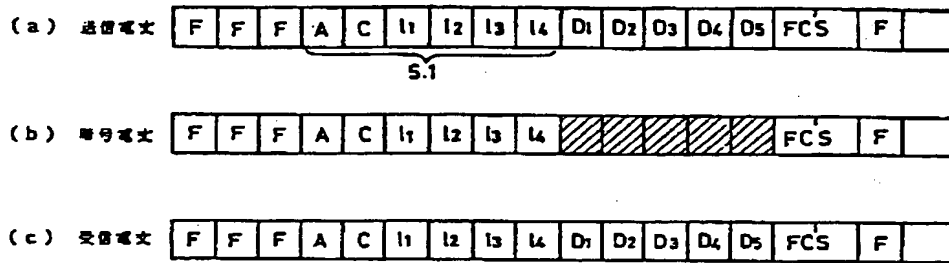
第1図のパターン検出器の構成図  
図 3



アドレス	データ
00	01
01	E4
02	18
⋮	⋮
FF	0B

(c)

第1図の暗号器の構成図  
図 5

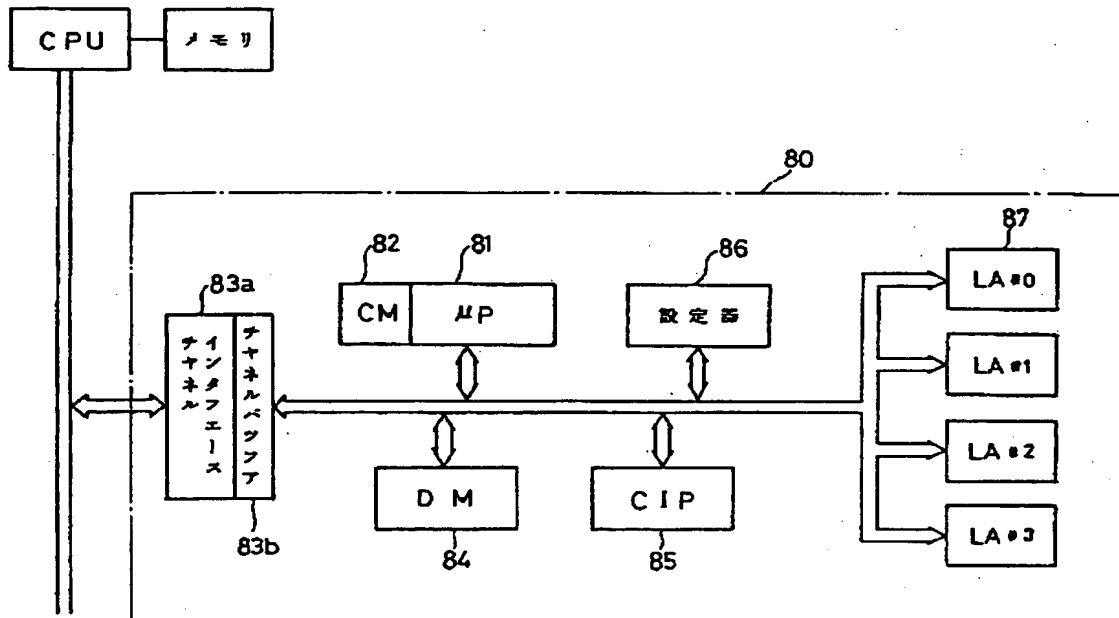


第1の実施例による送受信電文と番号電文  
第 6 図

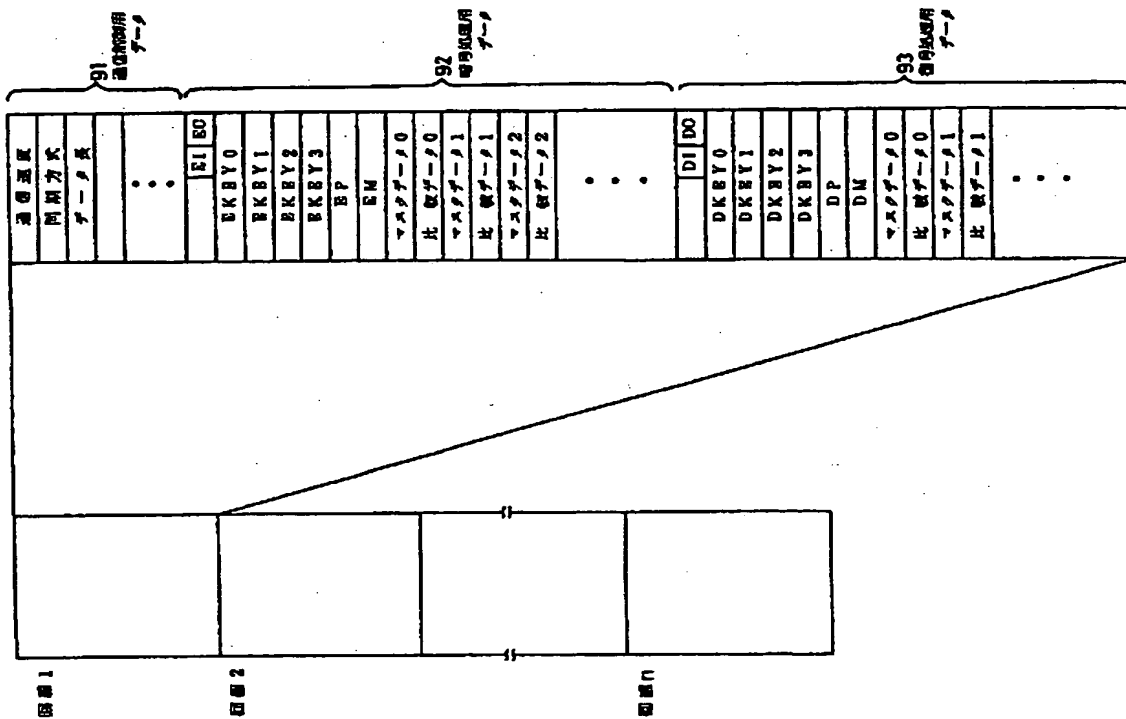
アドレス 0	FFH	55 (A)	0
1	01	00 (C)	0
2	70	20 (1)	0
3	00	00 (12)	0
4	01	00 (13)	0
5	00	00 (14)	1

アドレスM      比較アドレス      終了フラグ

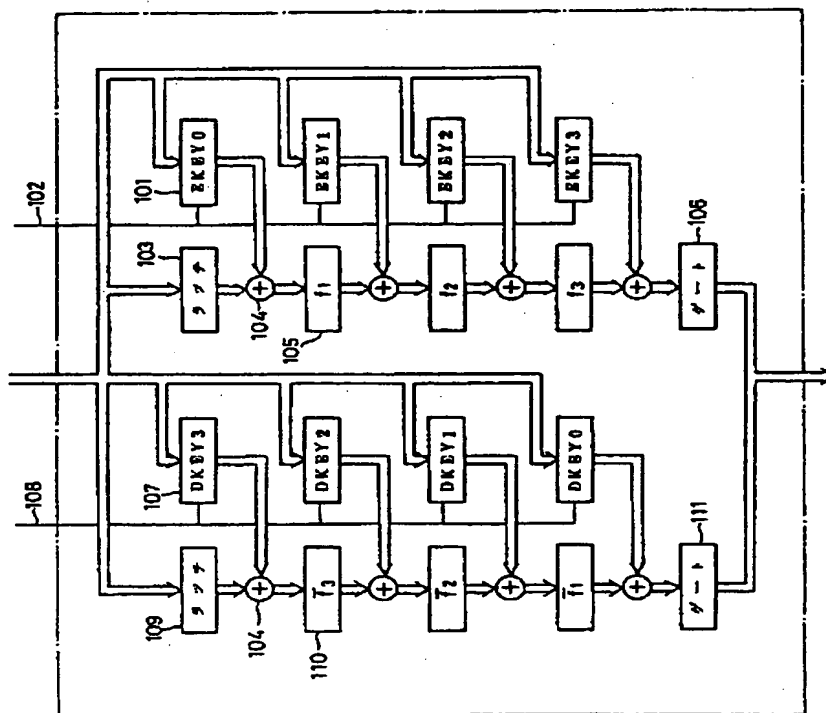
パターンデータメモリ例の説明図  
第 7 図



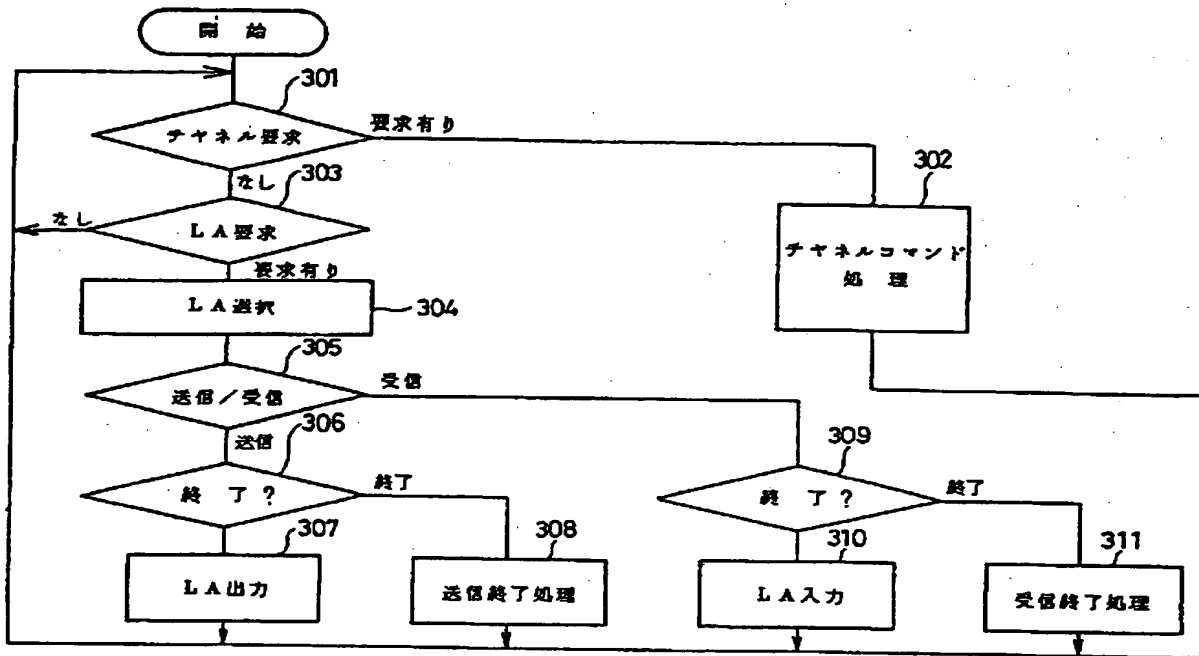
第2実施例の通信制御装置の構成図  
第 8 図



第 6 圖 鋼管の圧入による変位

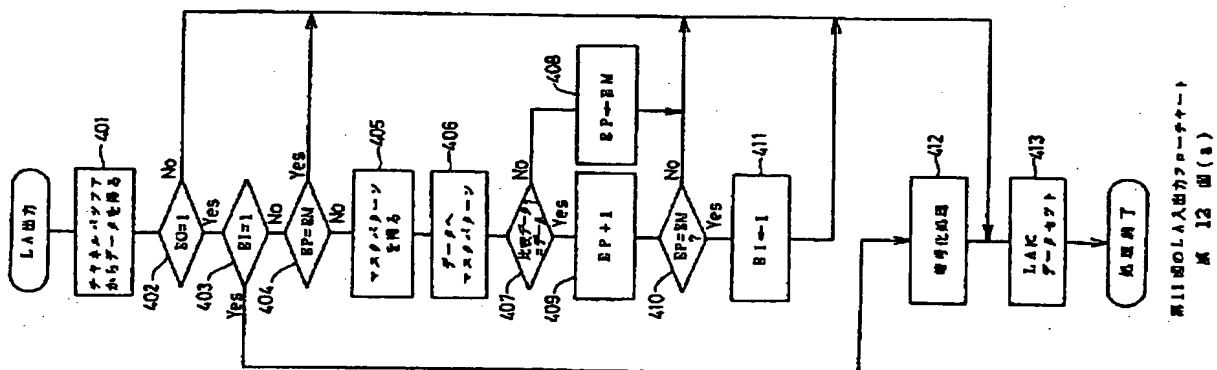


第 3 図の電圧/電流特性図

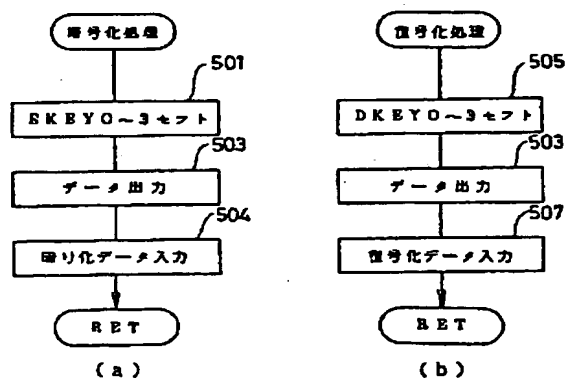
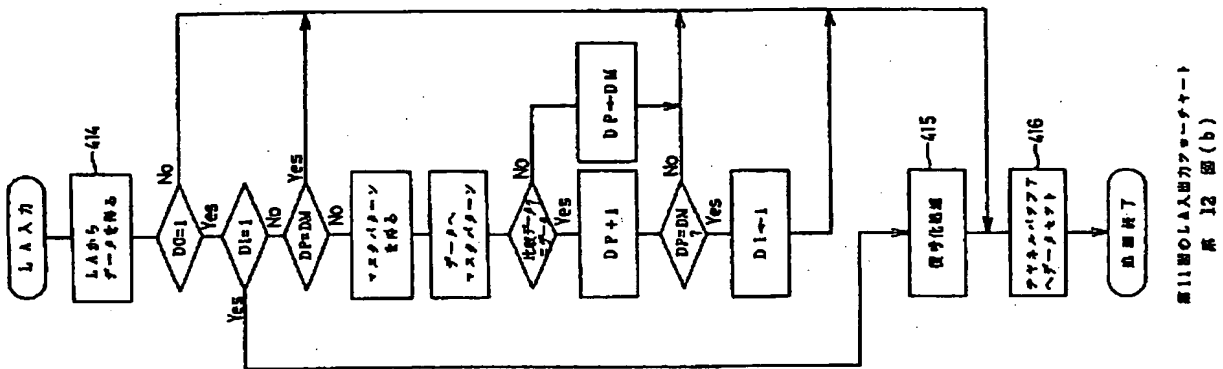


第 8 図の装置の制御フローチャート

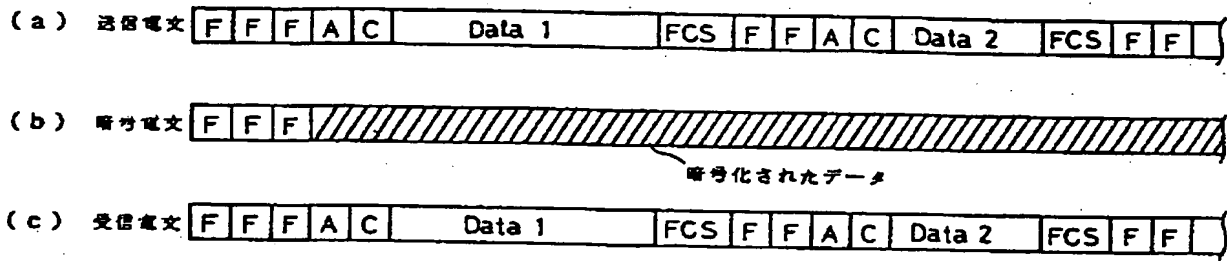
第 11 図



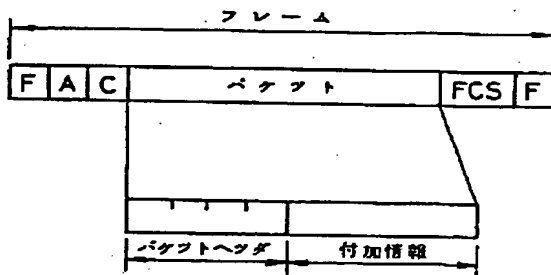
第 11 図の LA 出力フローチャート  
図 12 図 (a)



第12図の暗号化/復号化処理のフローチャート  
第 13 図



従来の送受信電文と暗号電文の構成図  
第 14 図



パケットの構成図  
第 15 図